National Aeronautics and Space Administration
Software Independent Verification and Validation Facility

Software Independent Verification and Validation

Handbook for Program Management

31 August 2000

Goddard Space Flight Center

1 INTRODUCTION

1.1 Overview

The Program Manager (PM) Handbook outlines the National Aeronautics and Space Administration (NASA) Goddard Space Flight Center (GSFC) Software Independent Verification and Validation (IV&V) Facility's approach for performing software IV&V on systems of the United States (US) government. The NASA Software IV&V Facility (henceforth referred to as the IV&V Facility) approach is based on risk mitigation early in, and throughout, a development program.

Included in the PM Handbook is a typical planning process for IV&V support. The culmination of the planning process is a detailed Memorandum of Agreement (MOA) (or its equivalent) which includes program milestones, IV&V deliverables, and time-based Technical and Status Reports.

1.2 Objectives

The objectives of the PM Handbook are to:

- Acquaint the PM staff with the capabilities and support of the Facility.
- Provide the PM staff with data on the benefits, limitations, and strengths of the Facility's IV&V program.
- Explain how the IV&V program provides the PM and the developer with documented analyses and results that identify both the positive and the deficient characteristics of the software.
- Inform the PM staff of the IV&V planning activities to address the Program risks.
- Advise the PM staff of the IV&V planning methodology to define an IV&V approach to fit within the Program cost, schedule, and technical and programmatic constraints.
- Specify the functions and responsibilities of the IV&V staff to support the PM.

1.3 Terminology

As used in this statement of work the following shall apply:

a. Program refers to an activity for which software is being generated that is subject to IA/IV&V.
b. The term Contractor refers to the prime contractor organization performing the IV&V of software generated by the above Program.

2   IV&V FACILITY IMPLEMENTATION APPROACH

The primary efforts of the IV&V activity are to provide the PM with assessments of the Program's software deliverables and processes for the development aspects of the Program. The IV&V activity, although independent of the developer, is an integral part of the overall development Program and is planned to mitigate the inherent risks associated with developing mission and safety critical software. The IV&V process defines a software engineering approach that ensures effective utilization of the available IV&V resources focused on mitigation of these Program risks. The IV&V approach is based on the following steps, which are detailed in subsequent paragraphs:

- Negotiate Initial MOA
- Assess the IV&V Need
- Tailor the IV&V Program
- Negotiate Final MOA
- Execute the IV&V Program
- Measure the IV&V Results/Impacts
- Focus Future IV&V Efforts

2.1   *Negotiate Initial MOA*

The IV&V Facility will assign a civil servant as the IV&V Program Manager (IPM) as soon as a program is identified. The IPM will be the point of contact during all subsequent interfaces with the PM while the MOA is negotiated, and, subsequently, the IV&V performance.

The IPM will negotiate a formal agreement with the PM or the PM's designated representative. This formal agreement will document the work to be performed and the resources required as described further in the following subsections.

2.1.1   Determine Type of Agreement

The IPM and PM will determine the form of the agreement to be utilized between the IV&V Facility and the program. Formal agreements may take the form of, but are not limited to, the following: a Memorandum of Agreement (MOA); Program Activity Commitment Terms (PACT); or a contract. If the PM does not have a strong preference, an MOA will be utilized. The agreement will contain but is not limited to the following areas:

- Purpose
- Scope
- Duration
- Schedule and Milestones
- Points of Contact
- Roles and Responsibilities
- Deliverables
- Tasks to be performed
- Resources
- Budget
- Signatures

2.1.2 Draft Initial MOA

The IPM will hold discussions with the PM to establish an initial set of services the PM desires of the IV&V Facility, any special resources (hardware or software) that may be required, and the time frame in which the work is to be performed. The purpose of this initial set of services is to get the IV&V program initiated as soon as possible, while a more complete understanding of the program's IV&V needs are assessed (see Section 2.2). Typically, this would include a minimum set of tasks to meet the needs of where the program currently is in the life-cycle, plus a criticality analysis and risk assessment to determine the complete set of tasks necessary.

2.1.3 Identify Team

Once the IPM has an initial scope of the work to be performed for the program, the IPM will coordinate with Facility management, financial personnel, civil servant peers, and possibly contractors to identify the team members necessary to perform the work for the customer.

2.1.4 Identify Tasks

In-depth discussions with the program will be conducted by the IPM and the team to further define the specific tasks to be performed. In the formal initial agreement, each individual task will be documented.

2.1.5 Identify Resources Required

Any special resources such as, but not limited to, hardware, software, communication lines, and travel will be determined and documented in the formal agreement. If IV&V Facility personnel are required by the agreement to be located at the customer site, the IPM will coordinate with the PM to make the necessary arrangements.

2.1.6 Define Cost

The IPM will coordinate with the team members and Facility management to determine the cost of the identified tasks, any special resources, and the General and Administrative costs associated with performing work at the IV&V Facility. These costs will be documented in the formal agreement.

2.1.7 Reach Initial MOA

Once the IPM and the PM reach agreement on the Initial MOA schedule, costs, and tasks, the IV&V Facility will send two signed copies of the Initial MOA to the PM for signature. The PM should sign both, send one back to the IV&V Facility, and keep the other.

2.1.8 Program Initiation

Once the agreement between the IV&V Facility and PM has been signed and the scope of the tasks and resources identified, the IPM will coordinate with the team to create an IV&V Program Master Plan (PMP) and any associated tasking mechanisms.

2.1.9   IV&V Program Master Plan

The IPM is responsible for the technical aspect of the IV&V effort and will prepare a program-specific PMP following the format of IEEE STD 1012-1986 (IEEE Standard for Software Verification and Validation Plans). A copy of this plan will be provided to the designated point of contact for the customer. A copy of this PMP will also be provided to the PM.

2.2   Assess the IV&V Need

The greatest challenge in providing IV&V support to a PM is the identification of the appropriate level of IV&V. The IV&V program must provide the status of the development products, assist in the mitigation of the software development program risks, provide timely inputs, and be cost effective. The Facility's IV&V program provides a unique approach to the assessment of the IV&V need which maximizes IV&V impact on the development Program at a minimum cost. Therefore, the Facility provides the guidelines for the assessment of the IV&V need based on the following:
- Software development Program risks
- Safety and mission criticality
- Schedule constraints
- Budget constraints

The primary inputs to the IV&V planning process are the development program characteristics and the associated risks and benefits. These characteristics include, but are not limited to:
- Program complexity
- Program criticality
- Development methodology
- Developer experience/history
- Development schedule

This process is known as the Criticality Analysis and Risk Assessment (CARA) process, and is described in Figure 2-1.
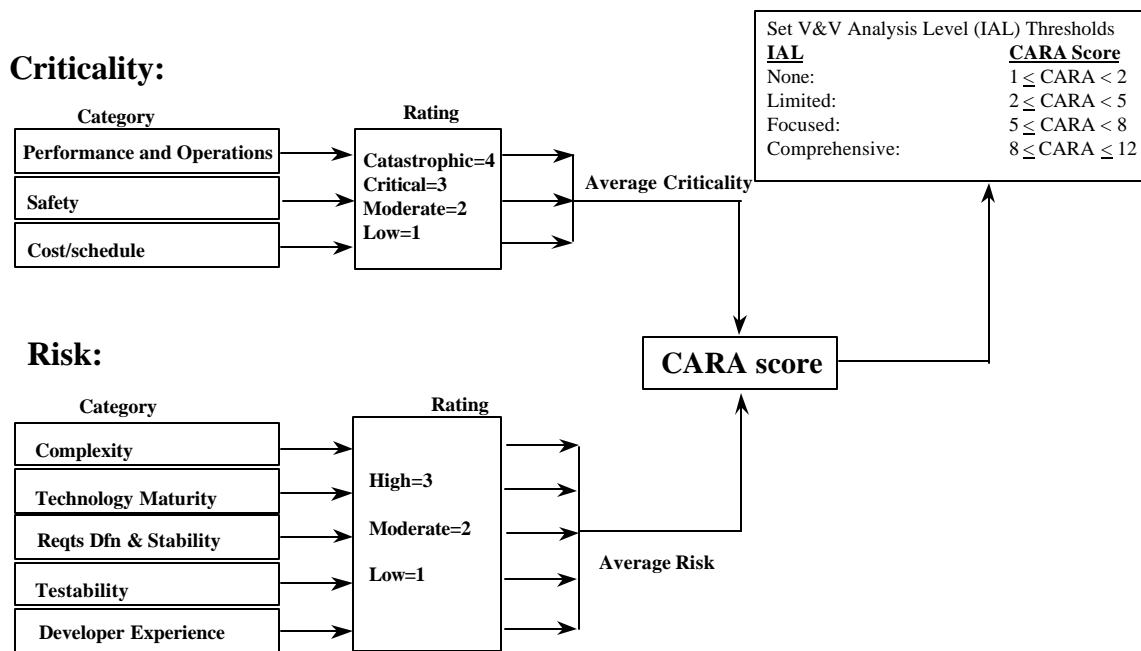
Criticality:

Category

| Performance and Operations |
| Safety |
| Cost/schedule |

Rating

Catastrophic=4
Critical=3
Moderate=2
Low=1

Average Criticality

Set V&V Analysis Level (IAL) Thresholds

IAL	**CARA Score**
None:	$1 \leq CARA < 2$
Limited:	$2 \leq CARA < 5$
Focused:	$5 \leq CARA < 8$
Comprehensive:	$8 \leq CARA \leq 12$

Risk:

Category

| Complexity |
| Technology Maturity |
| Reqts Dfn & Stability |
| Testability |
| Developer Experience |

Rating

High=3

Moderate=2

Low=1

Average Risk

CARA score

Figure 2-1 CARA Scoring Method

The schedule and budget constraints placed on the IV&V program are also considered in the planning process. The specific tasks, to be effective, must be completed in a timely manner with respect to the development schedule. The most beneficial IV&V program will be planned within the budgetary constraints of the PM, by tailoring the IV&V program to fit the specific development areas with the greatest risk and criticality (see Figure 2-2)

Specifications   Program goals   Dev plans/schedules   Program's IV&V budget

Criticality Analysis and Risk Assessment → **Estimate resource requirements** → **Acceptable?** — Yes → **IV&V Plan**

No

Revise scope:
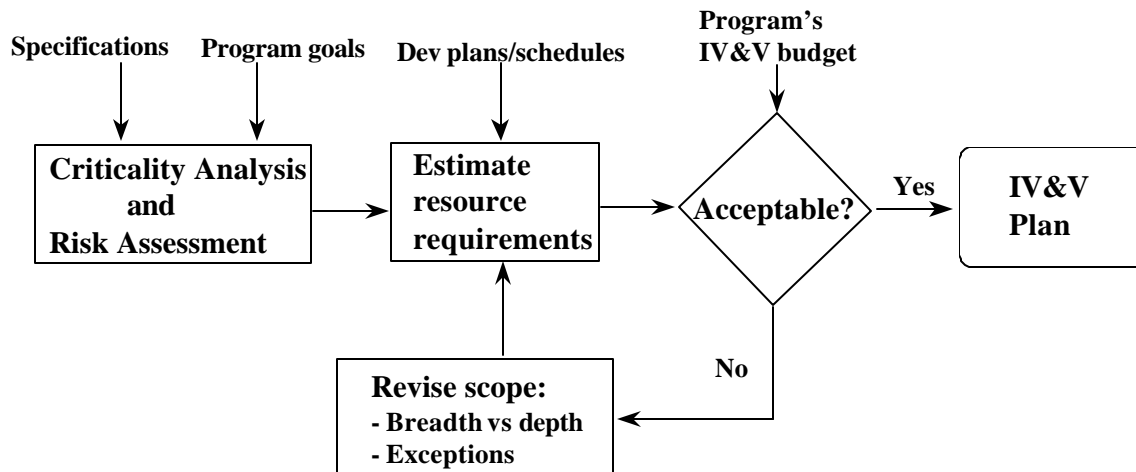- Breadth vs depth
- Exceptions

Figure 2-2 IV&V Scope

2.3   Tailor the IV&V Program

2.3.1   IV&V Tasks based on Need

The importance of providing a tailored IV&V effort to a specific PM cannot be overstated. The IV&V Facility approach allows the customization of our software engineering support program to ensure the PM that the critical assessments are provided during the appropriate phase or document release, and that the IV&V effort is targeted at the areas of most concern. The IV&V program is planned taking into account not only which of the tasks described in the following section 2.3.2 and Figure 2-3 should be performed, but also the "level" of each task based upon function CARA results. As an example, consider the processes employed in the performance of Requirements and interface analyses by IV&V. As can be seen in Table 2-1, requirements analyses take on different levels of rigor depending upon the IV&V analysis level applied (comprehensive, focused, or limited).

Table 2-1 Requirements Analyses

Analyses	Limited	Focused	Comprehensive
System Needs Validation	X	X	X
Traceability	X	X	X
Data/Adaptation Reqts	X	X	X
Testability	X	X	X
Data & Control Flow	X	X	X
Timing & Sizing	X	X	X
Key Algorithm Analysis		X	X
Examine prototypes of key algorithms		X	X
Alternative static analyses		X	X
Prototyping			X
Indep Timing/Sizing modeling			X
Formal Methods			X

2.3.2   IV&V Tasks

The IV&V analysis tasks for an individual program are defined in the MOA and the associated PMP (ref: Section 2.1.9). These tasks are divided into Phase Independent Tasks, and Phase Dependent Tasks (see Figure 2-3).
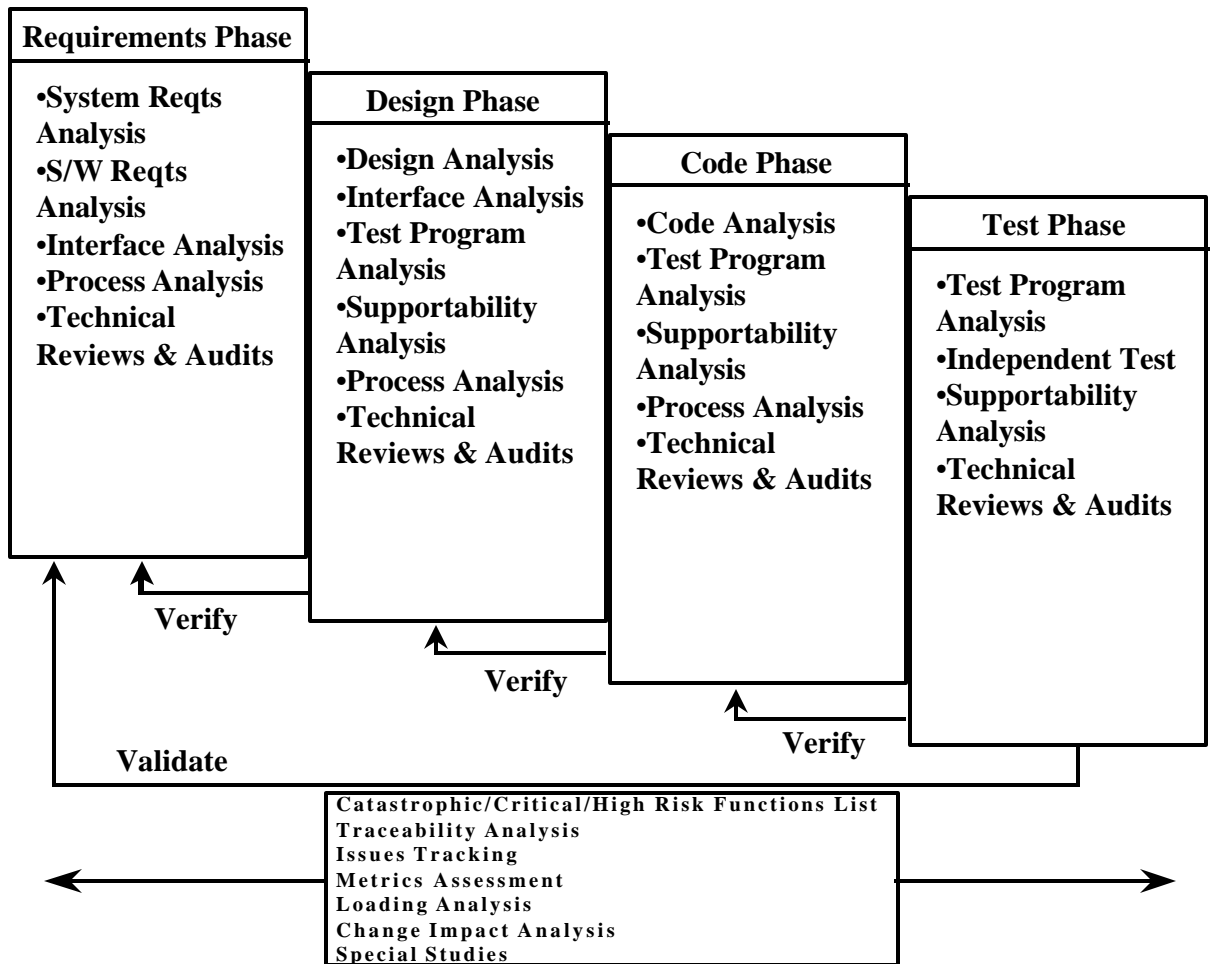
Figure 2-3 IV&V Tasks

2.3.2.1   Phase Independent Analyses

These tasks may be performed by analysts throughout the software life-cycle.

2.3.2.1.1   Criticality Analysis/Risk Assessment

The analyst will assess the software functions for criticality and risk. Criticality analysis will be based on the potential consequences associated with an error in or failure of the function. Risk assessment will be based on the likelihood of an error in or failure of the function. The analyst will document the assessment rationale and quantify both criticality and risk. The results of this analysis will be used to identify catastrophic, critical, high-risk (CCHR) functions.

This analysis will be performed on a frequency as specified in the PMP. The IPM will use this information for the redefinition of tasks and for the allocation of available resources. These changes, should they be recommended, will be reviewed with the PM.

2.3.2.1.2 Traceability Analysis

The analyst will analyze the successive stages in the development or progress of a requirement for correctness, consistency, completeness (sufficient detail to show compliance) and accuracy. This analysis is performed to ensure that system requirements are properly allocated to hardware and software requirements and that the allocated requirements are carried through to design, implementation and test.

2.3.2.1.3 Issues Tracking

The analyst will document all problems identified as a result of an analysis. The analyst will attempt to communicate and resolve problems with the development community informally. Informal resolution of problems will be documented. Problems which cannot be resolved with the developer at the informal, working level are candidates for elevation to an issue. If the problem is approved as an issue by the IPM, it will be documented as an issue and its status towards resolution updated and reviewed monthly. These issues will then be reviewed periodically with the Program.

2.3.2.1.4 Metrics Assessment

The analyst will utilize the program's software metrics and analyses results to identify deficiencies in the program's ability to comply with program requirements and schedules. The metrics may include processor sizing, processor timing, mass memory sizing, software development and test schedule, and software errors.

2.3.2.1.5 Loading Analysis

The analyst will perform a loading analysis on the associated computer system design. The analysis will examine processor and input/output loading during high-loading operations.

2.3.2.1.6 Change Impact Analysis

The analyst will assess that a proposed change is complete, meets the intent of the change, is necessary, and that all performance and operational usage impacts are identified. These assessments may pertain to flight rules, crew procedures, hardware, software and system requirements

2.3.2.2 Phase Dependent Analyses

These analyses are performed during a given software life-cycle phase (requirements, design, implementation, test).

2.3.2.2.1 Documentation Reviews

The analyst will review phase-dependent documentation for internal consistency, technical adequacy (e.g., requirements are unambiguous and testable), completeness, traceability to and consistency with higher level documentation, feasibility, and appropriate level of detail.

2.3.2.2.2 Process Analysis

The analyst will review process documentation to address the degree to which the documents meet the goals of the Data Item Description documents to which they were produced. The analyst may perform analyses in the following process areas: Software Interface Control, Software Configuration Management, Software Development, Software Test, and Software Integration. The analyst may assess the processes for implementation according to the associated plans and for appropriateness for the program environment at the time of the analysis.

2.3.2.2.3 Software Requirements Analysis

The analyst will perform analyses to ensure that the requirements form a solid basis for design and that the requirements are appropriate for the expected operational usage of the software. Documentation to be analyzed may include: System Segment Specifications, Software Requirements Specifications, Interface Requirements Documents, and System Segment Design Documents.

2.3.2.2.4 Interface Requirements Analysis

The analyst will analyze the Interface Control Documents (ICDs) to verify that the software requirements are correctly reflected in ICDs and to ensure that data and command initiation and response assumptions that are implied/specified within the ICDs are consistent with the specified requirements in the associated requirements documents.

2.3.2.2.5 Software Design Analysis

The analyst will perform analyses to assess the technical features and accuracy of the design, to analyze critical algorithms and control logic design (eg, determine performance, constraints, input/output discontinuities, feasibility), to evaluate modular interfaces and database design, to validate the testability of the design, and to review timing and sizing. Design phase documentation may include: Software Design Documents, Interface Design Documents, Software Product Specifications, and Database Design Documents.

2.3.2.2.6 Code Analysis

The analyst will perform analysis of the source code to verify correct, complete and accurate implementation of the software requirements and design specifications. The analyst will assess the maintainability and ability of the code to be properly and accurately reconfigured.

2.3.2.2.7 Analysis of Program's Verification and Validation Test Program

The analyst will analyze the development contractor's verification and validation testing program to ensure: complete and adequate test coverage; validity of the test definition; proper acceptance criteria; sufficient planning of tools, facilities, procedures, methods and resources; adequate planning for regression testing; and correct and complete traceability with test documents. The analyst will recommend specific changes to the developer's test plans and procedures whenever inadequacies are identified. Test documents to be analyzed may include: software test plans, software test descriptions, software test reports, design verification objectives, and design verification requirements.

The analyst will recommend selected tests to be monitored and specific test results to be independently analyzed. The analyst will document the results of program's formal test of requirements and the results of analysts verification of the requirement implementation.

2.3.2.2.8 Supportability Analysis

The analyst will perform analyses to verify that the software being developed is maintainable. The analyst may assess the Software User's Manuals, Computer System Operator Manuals, Firmware Support Manuals, and the Software Product Specifications. The analyst may assess the maintainability of the software and its ability to be properly and accurately reconfigured.

2.3.2.2.9 Technical Reviews

The analyst will develop a Software IV&V Report to be presented at each program major milestone review. Attendance, participation and reporting may be required for the following reviews: Integrated Design Review, System Requirements Review, System Design Review, Software Specification Review, Preliminary Design Review, Critical Design Review, Test Readiness Review, Functional Configuration Audit, Physical Configuration Audit, and Formal Qualification Review.

2.3.2.2.10 IV&V Testing

The analyst will recommend independent testing with the objective of verifying agreement between software and software specifications and demonstrating the software's adequacy to perform the mission. The proposed testing should complement rather that duplicate the developer's testing. The scope of the independent testing will be based on objectives, mission criticality, issues raised with the developer's test plans and procedures and available resources.

2.3.2.2.11 Certification of Readiness

The analyst will assess the readiness of the software to support each mission and submit an input to the program's Certification of Readiness process. The input

will be based on the appropriateness of the software configuration, adequacy of the certification activities, and the adherence to program processes. The Certificate of Readiness will be reviewed and signed by the IPM.

2.3.2.3   Technical Report

At the conclusion of an analysis activity, the analyst will prepare a technical report. The report will include (1) statement of the issues addressed or events reported during the analysis of design review and verification review; (2) summary of principle conclusions and/or major issues; (3) supporting technical detail or other information; and (4) recommendations for further action.

2.4   *Negotiate Final MOA*

The final MOA process will follow the identical process that was used in negotiating the initial MOA.

2.5   *Execute the IV&V Program*

The IV&V program is conducted independent of the developer to provide the PM an additional measure of the development Program status, and to reduce the development risk through the early detection of problems. The IV&V Facility provides a standardized, formal process for the evaluation of both the progress and the associated deliverables for each software development phase. The results of the IV&V Program (e.g., analyses, assessments, recommendations) for identified areas of risk, as well as for areas of sound software engineering progress, are provided to the PM to support the programmatic decisions necessary to ensure the successful fielding of a maintainable system.

A graphical description of the principal interfaces described in this section is included as Figure 2-4. The NASA IV&V Program Manager is responsible for prioritizing the Contractor work efforts and degree of analysis throughout the contract.

The IV&V function is an independent arm of the Program Manager for the assessment of selected CCHR software and its interfaces. Normal Contractor team interaction with the program will be through the various developer/design teams on an informal basis. This is the **primary data path** for conveying IV&V analyses results in a timely manner to the program. When IV&V recommendations are not accepted or implemented in a timely fashion, the option exists to use the formal path shown in Figure 2-4 to convey through the IV&V Program Manager recommendations to the program. This path is also used for more formal activity coordination (e.g., IV&V participation is requested by the program in a formal program review; formal delivery of an IV&V Position Paper). The interface point to the program for the NASA IV&V Program Manager is the Program's IV&V liaison. This liaison is sometimes a dedicated individual, but usually someone in the Program who has other duties, as well.
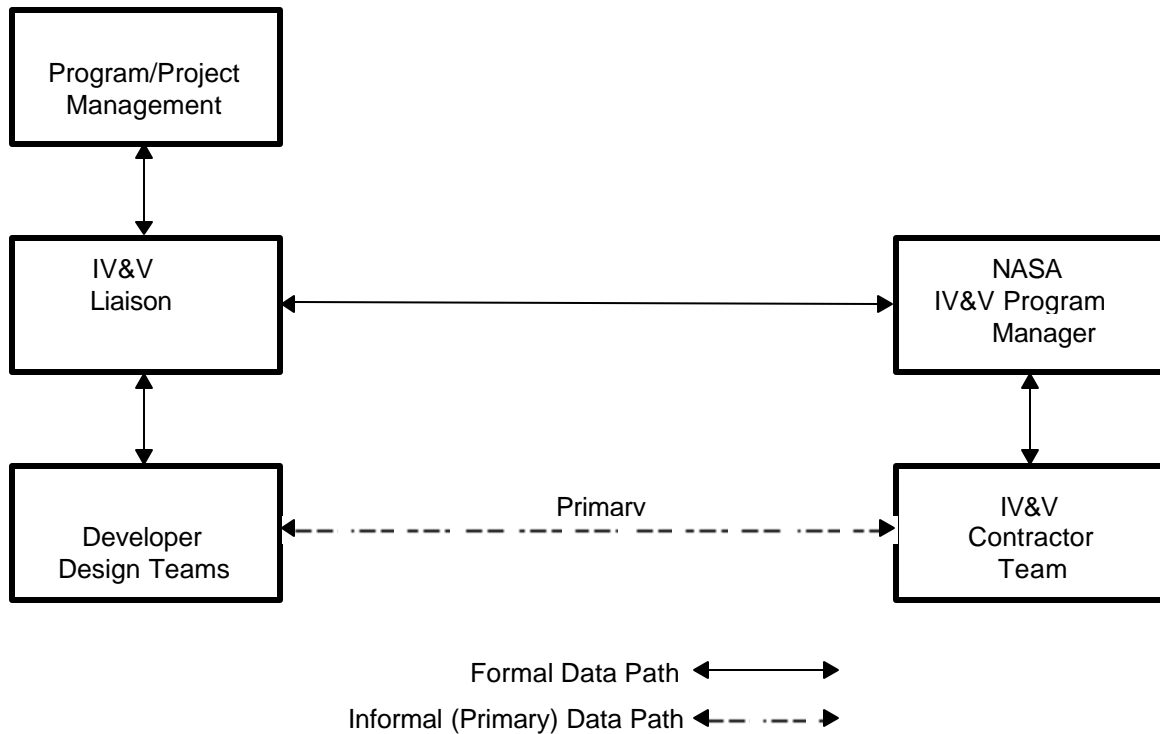
Figure 2-4 IV&V Reporting Responsibilities

The NASA IV&V Facility's paradigm for interfacing with a program in the performance of IV&V is as follows (Note: While none of the following are requirements, they do represent the typical IV&V Facility approach to IV&V of programs):

- Part of the Contractor staff is located at the developer's and the program's site to function as the "eyes, ears, and advocates" of the IV&V effort.
- Part of the Contractor staff is located at the IV&V Facility to promote synergism across programs and to allow access to Facility tools.
- The Contractor staff is composed of both program domain experts as well as software discipline experts.
- Management of the Contractor's program IV&V effort is located at the IV&V Facility to promote a close working relationship with NASA and to help affect the synergism described above.
- Contractor management is located at the IV&V Facility to promote timely and effective working relationships with the NASA staff and management.
- NASA IV&V Program Managers are located at the IV&V Facility.
- The program does not have a representative at the IV&V Facility.

2.6 *Measure the IV&V Results/Impacts*

The collection of metrics during performance of the IV&V program provides a data base of programmatic trend data and comparative programmatic status data. These types of data are used in identification of impending areas of Program development risk, determination of areas for future IV&V concentration, as well as assessment of the IV&V efforts in the identification of

significant problems (and thus, identification of areas for the Facility's ongoing process improvement efforts).

2.7 Focus Future IV&V Efforts

The initial IV&V PMP, developed as described in section 2.1.9, is based on the projected/anticipated risks as well as budget and schedule constraints. As the development program progresses, the IV&V plan is periodically updated based on the types of problems identified by execution of the IV&V program. These problems are assessed to concentrate the upcoming IV&V efforts on those areas representing the most potential benefit to the program.

2.8 Summary

The IV&V Facility provides the Program Manager with an industry leading approach, with the most efficient and effective utilization of resources, to ensure that a program receives the software engineering evaluation and support necessary to successfully deploy a system that meets its requirements, and does so within planned cost and schedule.

3 Benefits of the IV&V Facility

The core infrastructure that the IV&V Facility (Figure 3-1) utilizes to provide services to multiple programs allows for the synergistic sharing of resources. Through the efficient allocation of these resources, derived benefits such as lower cost, more rapid response and improved performance are realized by the programs.

The Facility is constantly striving to build upon the infrastructure capabilities in the following areas:

- Expertise: Our personnel base includes vast domain (eg, GN&C, C&DH) and software engineering discipline experience within NASA programs. This allows for the allocation of the proper skills as the program needs.
- Processes: Successful application of proven processes and continuous evaluation and improvement of these processes ensure that the Programs receive quality services.
- Tools: Software analysis tools and expertise in their usage are shared among the programs. This sharing results in a lower per-unit cost to the Programs. As needs are identified, specific tools are developed in-house and then shared across the Programs.
- Research: Our partnership permits the identification of needs by the services and development and demonstration of solutions by the Research element. Once proven, these new processes and tools are provided to the services for application within the Programs.
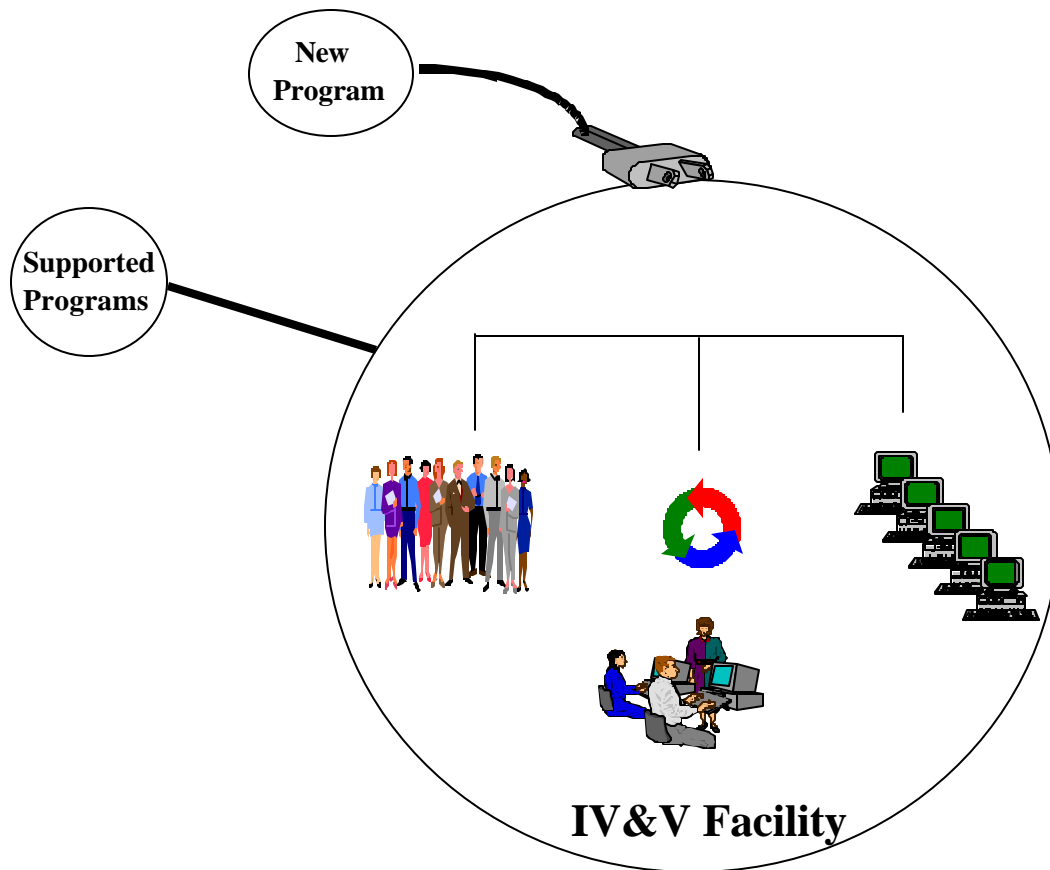

Figure 3-1 IV&V Facility Infrastructure Meets Customer Needs

Appendix A – Glossary

Analyst:

The Civil Service or contractor person assigned to perform a specific IV&V task.

Catastrophic/Critical/High Risk Software:

For the purposes of this SOW, software where a failure to execute or an inappropriate execution results in a catastrophic or critical hazard; or software where technical or developmental issues remain which threaten schedule milestones.

Complete:

All attributes fully defined to ensure full implementation. A specification is complete to the extent that all of its parts are present and each part is fully developed. Completeness is the measure of the degree of thoroughness of the translation and hence the measure of the adequacy of the level of detail to initiate the next phase in the development cycle.

Consistent:

Uniform and not in conflict with other requirements. A specification is consistent to the extent that its provisions do not conflict with each other or with governing specifications and objectives. Consistency is concerned with measuring the degree to which the specification of a given development phase is in agreement with the previous development phase.

Correctness:

Determines that the data entered, processed, and output by the application system is accurate and complete. Accuracy and completeness are achieved through controls over transactions and data elements. The control should commence when a transaction is originated and conclude when the transaction data has been used for its intended purpose.

Feasible:

A specification is feasible to the extent that the life cycle benefits of the system specified exceed its life cycle costs. Feasibility also includes verifying that a system can be developed that satisfies the specified requirement with respect to resource engineering.

Independent Verification and Validation (IV&V):

A process whereby the products and processes of the software development life cycle phases are independently reviewed, verified, and validated by an organization that is neither the developer nor the purchaser of the software. IV&V differs from Verification and Validation (V&V) principally in that it is performed by an independent organization.

IV&V Program Manager:

The Civil Service person designated as responsible for the performance of the IV&V activities for a particular program.

Maintainable:

The software is maintainable to the extent that it can be modified as necessary to correct problems or to respond to changing requirements. Attributes that may affect the maintainability include complete, concise, and readable documentation of design, operations, and support as well as modular software implementation.

Program:

The technical, financial, and management elements of the IV&V customer.

Validation:

The process of evaluating software at the end of its software development process to ensure compliance with software requirements. This process ensures that the software system performs to the customer's expectations under operational conditions.

Verification:

The process of determining whether or not the products of a given phase of the software development cycle fulfill the requirements established during the previous phase.